UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Richmond Division

NOREEN SMITH, Individually and on behalf of all others similarly situated,

Plaintiff,

v. **Case No. 3:23-cv-510**

GENWORTH FINANCIAL, INC.,

SERVE: **Corporation Service Company, Registered Agent**
100 Shockoe Slip, Fl 2
Richmond, VA 23219

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Noreen Smith ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself, and on information and belief as to all other matters, brings this Class Action Complaint against Defendant Genworth Financial, Inc. ("Defendant" or "Genworth") and in support thereof alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of herself and all other individuals ("class members"), totaling more than 2.7 million[1] people who had their sensitive personal identifiable information ("PII") accessed and hacked by malicious, unauthorized third parties that accessed and removed the PII as early as May 27, 2023 from systems used by Defendant (the "Data Breach").[2]

[1]https://www.genworth.com/moveit.html (last accessed August 11, 2023).
[2] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-

2. Defendant markets mortgage, long-term care insurance, life insurance, and other insurance and financial products, primarily to individual consumers.[3] As part of its business, Defendant collects consumer data, including consumers' social security number, first and last name, date of birth, zip code, state of residence, full address, and preferred mailing address.[4]

3. Defendant touts the safety and security of its services on its website. For instance, Defendant's website warrants to consumers that:

> [W]e use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards.[5]

4. These comments assuring consumers that its services are safe apply to third-party services that Defendant uses in the ordinary course of its business, such as MOVEit. Defendant explicitly states that:

> We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated.[6]

5. Contrary to its assurances to consumers, however, Defendant lacked adequate systems and procedures for maintaining, safeguarding, and protecting highly sensitive PII entrusted to it. Specifically, on or about June 24, 2023, Defendant published a notice on its website

---

researchers-say-2023-06-02/ (last accessed August 8, 2023); https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last accessed August 8, 2023).

[3] GENWORTH FINANCIAL SERVICES, INC., *SEC Form 10-K* (FY 2022).

[4] GENWORTH FINANCIAL SERVICES, INC., *SEC Form 8-K* (June 16, 2023); https://www.genworth.com/moveit.html (last accessed Aug. 10, 2023).

[5] https://www.genworth.com/online-privacy-policy.html (last accessed Aug. 10, 2023).

[6] *Id*.

directed to class members, including Plaintiff, informing them that their highly sensitive PII was compromised in the Data Breach that impacted the MOVEit software.[7]

6. Based on this website notice, Defendant learned of the Data Breach on June 16, 2023, but inexplicably waited over a week before posting its notice.[8] Upon information and belief, Plaintiff alleges that few of Defendant's consumers read or were aware of this notice, and failed to learn about the breach until receiving letters from Defendant more than a month after it had learned of the breach.[9]

7. It has been reported that the Data Breach was a ransomware attack conducted by a notorious ransomware group, C10p, which claims to have committed the Data Breach.[10]

8. Defendant owed a non-delegable duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure.

9. Defendant could have prevented the Data Breach by properly vetting and monitoring its systems and third-party service providers, including MOVEit.

10. By way of example, had Defendant limited the customer information that it shared with their vendors and business associates and/or employed reasonable measures to assure their vendors and business associates implemented and maintained adequate data security measures and protocols to secure and protect Plaintiff's and class members' data, the breach could have been prevented.

---

[7] https://www.genworth.com/moveit.html (last accessed Aug. 10, 2023).
[8] *Id*.
[9] *See* https://www.genworth.com/moveit.html ("UPDATE – August 9: Many Genworth customers and some agents are currently receiving written letters from both PBI, a Genworth vendor (logo below), and Genworth regarding the MOVEit Security event. These letters are legitimate.")
[10] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last accessed Aug. 10, 2023).

11. Plaintiff and class members entrusted Defendant with, and allowed Defendant to gather, their highly sensitive PII. They did so in confidence, and they had the legitimate expectation that Defendant would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

12. Trust and confidence are key components of Plaintiff's and class members' relationship with Defendant. Without it, Plaintiff and class members would not have provided Defendant with, or allowed Defendant to collect, their most sensitive information in the first place. To be sure, Plaintiffs and class members relied upon Defendant to keep their information secure, as it is required by law to do.

13. Defendant breached its non-delegable duties to class members by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII entrusted to it from unauthorized access and disclosure, including by ensuring its vendors and business associates had secure services, processes and procedures in place to safeguard PII that Defendant shared with those third-parties.

14. As a result of Defendant's breaches of its non-delegable duties and obligations, the Data Breach occurred and Plaintiff's and class members' PII was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy these failings and their consequences. Plaintiff thus brings this complaint on behalf of herself and all similarly situated individuals whose PII was exposed as a result of the Data Breach.

15. Plaintiff, on behalf of herself and all other class members, asserts claims for negligence, negligence per se, invasion of privacy, unjust enrichment, and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other

relief authorized by law.

PARTIES

A. Plaintiff

16. Plaintiff is a resident and citizen of the state of South Carolina and resides in Beaufort, South Carolina.

17. Plaintiff received a letter from Defendant dated July 31, 2023, informing her of the Data Breach but not specifying which information was compromised.

18. Ten days prior, on July 21, 2023, Plaintiff received a letter from Pension Benefit Information, LLC ("PBI") stating that it provides services to Defendant, and was impacted by the Data Breach. Specifically, the letter explained as follows:

> On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBl utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed th is review.

The letter stated further that Plaintiff's name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), and policy/account number were compromised in the Data Breach.

19. Prior to retaining counsel for claims related to the Data Breach, Plaintiff spent at least an hour monitoring her accounts for fraudulent activity and identity theft. She will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

B. Defendant

20. Defendant Genworth Financial, Inc. is a Delaware corporation, with its principal place of business in Richmond, Virginia.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendant.

22. Discovery will show that there are greater than 100 putative class members and greater than two-thirds of them are diverse from Defendant.

23. The Court has general personal jurisdiction over Defendant because it maintains its headquarters and principal places of business in this judicial District and Division (i.e., in Richmond, Virginia), have minimum contacts with the Commonwealth of Virginia, and conducts substantial business in the Commonwealth of Virginia.

24. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in the Commonwealth of Virginia, Defendant maintains physical offices and principal places of business in this District and Division, and because Defendant conducts a substantial part of its business here.

FACTUAL ALLEGATIONS

A. Overview of Defendant

25. Defendant states that "[i]n today's increasingly digital world, protecting our own data – and that of our customers and business partners – is essential. Genworth recognizes the

significant operational risks, including risks of losses, from cyberattacks and the importance of a strong cybersecurity program for effective risk management."[11]

26. In recognition of these security concerns, Defendant represents that it has a robust data security apparatus, claiming that[12]:

> Our program employs various controls and policies to secure our operations and information including monitoring, reporting, managing, and remediating cybersecurity threats. Key features of the program include access controls, security training, dedicated security personnel, security event monitoring, and when necessary, consultation with third-party data security experts.
>
> Our IT security program, which is regularly updated to align with best practices and industry guidelines, includes:
>
> - Written IT policies and standards designed to guard the integrity of our institutional, commercial, and private consumers' personal information
> - Regular external and internal reviews of our data protection practices
> - A robust suite of IT security products that enable us to manage cybersecurity risk within the organization and alternate sites where business is conducted[.]

27. Defendant further warrants that it has specific "procedures for reporting and responding to potential security incidents as well as determining applicable disclosure requirements."[13]

28. Throughout its website, Defendant reiterates these promises, repeatedly stating that it is keenly aware of data privacy risks and has adequate procedures and process in place to prevent them, such as its statements below:

- "Working to protect your personal information is one of our promises that enables us to help millions of policyholders secure their financial lives, families, and futures."[14]

---

[11] GENWORTH FINANCIAL SERVICES, INC., *2022 Sustainability Report* at p. 31, https://pro.genworth.com/riiproweb/productinfo/pdf/665101C.pdf (May 16, 2023).
[12] *Id.*
[13] *Id.*
[14] https://www.genworth.com/fraud-and-information-protection.html (last accessed Aug. 10, 2023).

- "At Genworth, we have implemented technical, physical, and process safeguards to maintain the confidentiality of your information."[15]

- "Genworth uses reasonable administrative, physical and electronic security measures to protect against possible loss, misuse or alteration of Permitted Information or content posted on Bulletin Boards."[16]

- "When you provide information to us on our websites, we use encryption and authentication tools to protect that information after it gets to us."[17]

- "Once we receive your information, we use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards."[18]

- "We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated."[19]

- "In order to protect your personal data, we maintain physical, electronic and procedural safeguards. We review these safeguards regularly in keeping with technological advancements. We restrict access to your personal data. We also train our employees in the proper handling of your personal data."[20]

29. Based on the foregoing, Defendant was aware that it owed non-delegable duties to Plaintiff and class members to keep their PII safe and secure, which includes duties to ensure that all information Defendant collects, stores and/or transfers is secure, and that any associated entities with whom Defendant shared information maintained adequate and commercially reasonable data security practices to ensure the protection of PII within Defendant's possession.

---

[15] *Id*.
[16] https://www.genworth.com/terms-of-use.html (last accessed Aug. 10, 2023).
[17] https://www.genworth.com/online-privacy-policy.html (last accessed Aug. 10, 2023).
[18] *Id*.
[19] *Id*.
[20] GENWORTH FINANCIAL SERVICES, INC., *Privacy Policy* at p. 1, https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last accessed Aug. 10, 2023).

30. Discovery will show that through Defendant's provision of its services, it obtains possession of customers'—including Plaintiff's and class members'—highly sensitive PII. Thus, in the regular course of its businesses, Defendant collects and/or maintains the PII of consumers such as Plaintiff and class members, and stores that information digitally in the regular course of business.

31. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII was compromised in the Data Breach, Plaintiff's and class members' PII was transferred using MOVEit service and/or they otherwise entrusted to Defendant their PII, from which Defendant profited.

32. Yet, contrary to Defendant's website representations—by virtue of Defendant's admissions that it experienced the Data Breach which revealed the PII of more than 2.7 million individuals—Defendant did not have adequate measures in place to protect and maintain sensitive PII entrusted to it, or to ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected consumers' PII that Defendant shared with third-party vendors such as through Defendant's use of MOVEit.[21] Instead, Defendant's websites wholly fail to disclose the truth: that Defendant lacks sufficient processes to protect the PII entrusted to it.

B. The Data Breach

33. Defendant posted an explanation of the Data Breach on its website that states as follows[22]:

> PBI [, a Genworth contractor,] advised Genworth of a security event connected to the vulnerability in the MOVEit file transfer software that PBI uses. The estimated occurrence of the event was May 29, 2023, and the estimated end date was May 30,

[21] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html html (last accessed Aug. 10, 2023).
[22] https://www.genworth.com/moveit.html html (last accessed Aug. 10, 2023).

> 2023. On June 2, 2023, PBI implemented the patches (or fixes) provided by Progress Software, the producer of MOVEit.
>
> On June 16, 2023, PBI advised Genworth that specific Genworth files containing policyholder and agent information were compromised due to a security event that took advantage of a vulnerability identified in the widely-used MOVEit file transfer software that PBI uses …. The event included personal information for approximately 2-5-2.7 million individuals who are either customers or insurance agents. The personal information accessed included life insurance, individual and group long-term care insurance, and annuity customers.
>
> For customers, the exposed information includes one or more of the following: social security number, first and last name, date of birth, zip code, state of residence, policy number, the role of the individual (ex. Annuitant, Joint Insured, Owner, etc.), and general product type. If deceased, the exposed information also includes the city and date of death, along with the source of that information.
>
> For agents, the exposed information includes social security number, first and last name, date of birth, full address, and a preferred full address. If deceased, the exposed information also included date of death and the source of that information.

34. Based on Defendant's statement on its website, Defendant learned of the Data Breach on June 16, 2023, but inexplicably waited over a week before posting a notice to class members that their highly sensitive PII were compromised thereby. Further, upon information and belief, Plaintiff alleges that few of Defendant's consumers read or were aware of this notice, and failed to learn about the breach until receiving letters from Defendant more than a month after it had learned of the breach.[23]

35. Defendant's letter states that the breach originated through a compromise of the MOVEit service. MOVEit is a "managed file transfer software" that companies—such as Defendant—use to transfer files.[24] Defendant—and/or their vendors such as PBI—use MOVEit in

---

[23] *See* https://www.genworth.com/moveit.html html (last accessed Aug. 10, 2023) ("UPDATE – August 9: Many Genworth customers and some agents are currently receiving written letters from both PBI, a Genworth vendor (logo below), and Genworth regarding the MOVEit Security event. These letters are legitimate.")

[24] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last accessed August 10, 2023).

the regular course of their business.

36. Thus, the Data Breach resulted from Defendant's failure to adequately protect and safeguard the highly sensitive PII entrusted to it, including by ensuring its vendors and business associates had secure services, processes and procedures in place to safeguard PII that Defendant shared with those third-parties.

37. As noted above, it is believed that the Data Breach was a ransomware attack conducted by C10p, which itself claims to have committed the Data Breach.[25]

38. Through its hack of MOVEit, C10p claims to have stolen PII and protected health information ("PHI") from over 550 organizations and 37 million individuals, including U.S. schools, the U.S. public sector, and the U.S. private sector.[26]

39. C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[27]

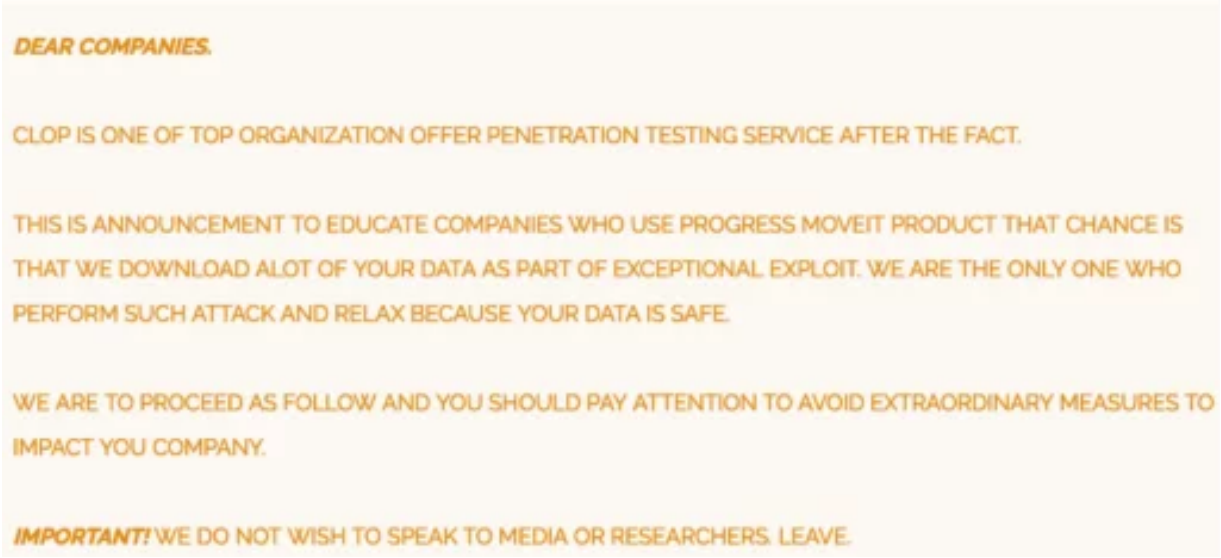
40. It has been reported that C10p has requested unspecified ransom from organizations impacted by MOVEit breaches in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI.

41. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[28]

---

[25] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last accessed August 11, 2023).
[26] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last accessed August 11, 2023).
[27] *Id*.
[28] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last accessed August 11, 2023).

42. C10p posted a statement on its website demanding ransom from all companies impacted by the MOVEit breach, which includes the present Data Breach, stating that if they refused to pay the ransom, C10p would post the sensitive PII and PHI stolen from Defendant's systems on the dark web[29]:



DEAR COMPANIES.

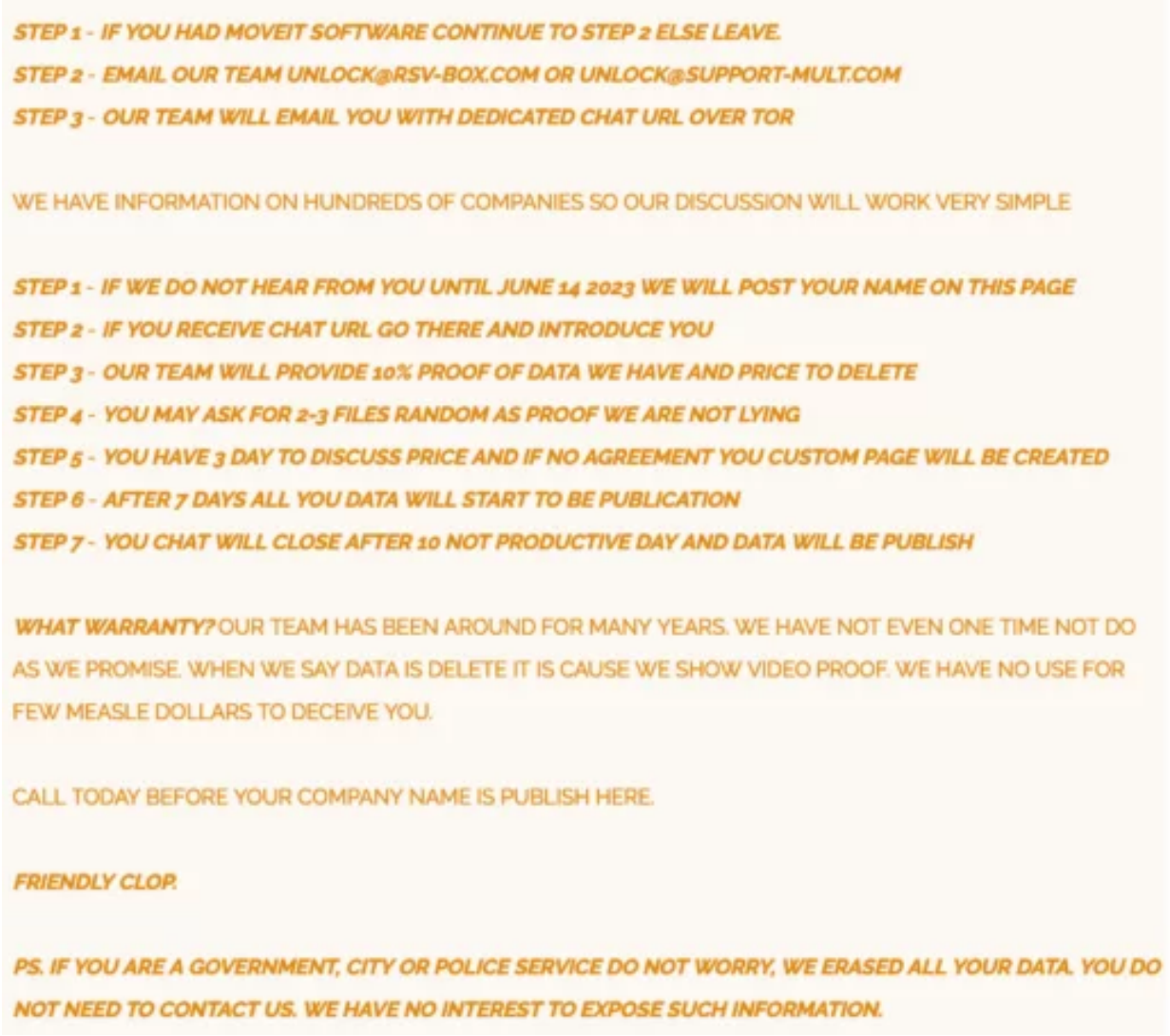
CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

[29] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/



STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

43. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiff's and class members' sensitive PII is irrefutably in the possession of known bad actors. Furthermore, based on C10p's statement above, Plaintiff's and class members' PII may have already been published, which places them at imminent risk that their data will be misused.

44. As explicitly acknowledged and stated on its own website, Defendant owed non-delegable duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access

and disclosure, and to promptly notify individuals of any breach involving their information. Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and disclosure, including by ensuring its vendors and business associates—such as PBI and the MOVEit service—had secure services, processes and procedures in place to safeguard PII that Defendant shared with those third-parties.

45. There were multiple things Defendant could have done—and was obligated to do—to ensure PBI (and the MOVEit service) had secure services, processes, and procedures in place to safeguard PII that Defendant provided to it, which would have prevented the Data Breach, but Defendant simply opted not to do them. For instance, as one leading cybersecurity expert explained, Defendant should have done the following when utilizing MOVEit. These steps, alongside others, could have ensured the sensitive PII Defendant transferred through MOVEit remained secure and free from data breach:

- "MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (e.g., access gateways secured by MFA) or simple allowlists and blocklists."[30]
- "If you run MOVEit within your organization, ensure that the database runs as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the adversary only gains initial access

[30] https://securityscorecard.com/blog/three-steps-to-avoid-moveit-exploit/ (last accessed August 11, 2023).

to the database server and user."[31]

Defendant also could have employed (either internally or through third parties) competent professionals to act as 24/7 "eyes on glass." Providers of managed security services, also referred to as "managed detection and response" ("MDR") employ a sophisticated series of artificial and human intelligence to monitor for signs that a breach is underway.

46. Either on its own or through the use of a qualified third-party vendor, Defendant could and should have been monitoring its own systems and repositories for indications of compromise ("IOCs.") It has been reported, for example, that the MOVEIT vulnerability was exploited by C10p "injecting" SQL computer code in order to execute a series of commands that ultimately resulted in the exfiltration of data. But companies have an obligation to monitor their systems for the execution of unauthorized code. If Defendant had had appropriate monitoring in place, it could have detected, and prevented this attack.

47. Companies who were using appropriate managed security detected the MOVEIT vulnerability as early as May 27, 2023, and were able to take steps to prevent the large-scale exfiltration of consumers' sensitive information. For instance, on May 27, 2023, as part of C10P's attack of MOVEit, "Akamai researchers detected exploitation attempts against one of Akamai's financial customers — an attack that was blocked by the Akamai Adaptive Security Engine."[32] Thus, services were available for Defendant to detect the Data Breach and prevent large scale exfiltration of PII entrusted to Defendant, but Defendant simply failed to appropriately implement these services. Furthermore, it does not take cybersecurity expertise to know Defendant should not have maintained—or allowed the maintenance of—2.7 million consumers' PII on MOVEit

[31] *Id*.
[32] https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware (last accessed August 11, 2023).

software, where it was a sitting duck waiting for a cyberattack such as the Data Breach. In sum, there were plenty of technologies and processes readily available that Defendant could have utilized to prevent the Data Breach, but Defendant failed to do so.

C. Defendant Knew that Criminals Target PII

48. At all relevant times, Defendant knew, or should have known, its clients'—such as Plaintiff's and all other Class members'— PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendant should have anticipated and guarded against.

49. PII is a valuable property right.[33] The value of PII as a commodity is measurable.[34] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[35] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[36] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[33] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[34] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[35] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[36] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

50. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

51. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[37]

52. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII Has Grave and Lasting Consequences for Victims

53. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, start new utility accounts, and incur charges and credit in a person's name.[38]

[37] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[38] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

54. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[39] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[40]

55. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[41]

56. Identity theft is not an easy problem to solve. In a survey, the Identity Theft

---

[39] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[40] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[41] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).

Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[42]

57. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

58. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[43]

59. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[44]

60. It is within this harsh and dangerous reality that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[42] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

[43] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[44] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

E. Damages and Harm Sustained by Plaintiff and the Other Class Members

61. As a direct and proximate result of Defendant's failures alleged above, Plaintiff and Class members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

62. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Defendant's negligent security processes and procedures and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff and the Class; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

63. For the reasons mentioned above, Defendant's conduct, which directly and proximately caused the Data Breach, caused Plaintiff and members of the Class these significant injuries and harm.

64. Plaintiff brings this class action against Defendant for its failure to: (1) properly secure and safeguard PII; (2) ensure that proper security measures were in place to protect PII; (3) ensure that is vendors and business associates had secure services, processes and procedures in place to safeguard PII that Defendant shared with those third-parties; and (4) provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII had been compromised.

CLASS ALLEGATIONS

65. Plaintiff brings this action on behalf of herself and the following classes:

> Nationwide Class: All residents of the United States whose PII was compromised as a result of the Data Breach.
>
> South Carolina Subclass: All residents of South Carolina whose PII was compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the

Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and its current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

66. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 2.7 million members who are geographically dispersed.

67. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the class members she seeks to represent.

68. **Adequacy**: Plaintiff's interests are aligned with the Class she seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

69. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendant's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

70. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII;

c. Whether Defendant breached its duties to protect Plaintiff's and class members' PII;

d. Whether Plaintiff and all other class members are entitled to damages and the measure of such damages and relief.

71. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the South Carolina Subclass)

72. Plaintiff realleges and incorporates by reference the above paragraphs as if fully set forth herein.

73. Defendant owed duties to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII in Defendant's possession, custody, or

control, including non-delegable duties to safeguard that PII. This duty could not be delegated to Defendant's vendors and business associates; rather, Defendant had an independent obligation to control all environments into which it placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

74. Defendant owed duties to Plaintiff and class members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and class members' PII within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

75. Defendant owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the PII.

76. Defendant knew the risks of collecting and storing Plaintiff's and all other class members' PII and the importance of maintaining secure systems and ensuring its vendors and business associates with whom Defendant shared consumers' PII—such as PBI through MOVEit—had secure services, processes and procedures in place to safeguard that PII. Defendant knew of the many data breaches that targeted PII, especially SSNs, in recent years.

77. Given the nature of Defendant's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

78. Defendant breached its duties in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and class

members' PII;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates such as PBI (and the MOVEit service);

e. Failing to adequately monitor, evaluate, and ensure the security of PBI's network and systems;

f. Failing to recognize in a timely manner that Plaintiff's and class members' PII had been compromised; and

g. Failing to timely and adequately disclose that Plaintiff's and class members' PII had been improperly acquired or accessed.

79. It was reasonably foreseeable to Defendant that failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to control, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols to ensure that all software and hardware systems into which it placed consumers' data were protected against the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII.

80. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII would not have been compromised.

81. As a result of Defendant's above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class

members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by Defendant; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the South Carolina Subclass)

82. Plaintiff realleges and incorporates by reference paragraphs 1 through 71 as if fully set forth herein.

83. Defendant's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

84. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other class members' PII and not complying with applicable industry standards, including by failing to control all environments into which it placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach

involving PII including, specifically, the substantial damages that would result to Plaintiff and the other class members.

85. Defendant's violations of Section 5 of the FTCA constitute negligence *per se*.

86. Plaintiff and class members are within the class of persons that Section 5 of the FTCA were intended to protect.

87. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA were intended to guard against.

88. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII to unauthorized individuals.

89. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by Defendant; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach;

and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT III
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the South Carolina Subclass)

90. Plaintiff realleges and incorporates by reference paragraphs 1 through 71 as if fully set forth herein.

91. Plaintiff and class members had a reasonable expectation of privacy in the PII that Defendant failed to safeguard and allowed to be accessed by way of the Data Breach.

92. Defendant's conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

93. By intentionally and/or knowingly failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and class members.

94. Defendant knew that an ordinary person in Plaintiff's and a class member's position would consider Defendant's intentional actions highly offensive and objectionable.

95. Defendant invaded Plaintiff and class members' right to privacy and intruded into Plaintiff's and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

96. Defendant intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

97. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

98. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

99. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of herself and the Class.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the South Carolina Subclass)

100. Plaintiff realleges and incorporates by reference paragraphs 1 through 71 as if fully set forth herein.

101. Plaintiff and class members have both a legal and equitable interest in their PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

102. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and class members. Defendant also benefitted from the receipt of Plaintiff's and class members' PII.

103. As a result of Defendant's failure to safeguard and protect PII, Plaintiff and class members suffered actual damages.

104. Defendant should not be permitted to retain the benefit belonging to Plaintiff and class members because Defendant failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

105. Defendant should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the South Carolina Subclass)

106. Plaintiff realleges and incorporates by reference paragraphs 1 through 71 as if fully set forth herein.

107. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Defendant on the other hand, concerning the Data Breach and Defendant's failure to protect Plaintiff's and class members' PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendant has performed and are adhering to all data

privacy obligations as required by law or otherwise to protect Plaintiff's and class members' PII from unauthorized access, disclosure, and use.

108. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policy and whether it failed to adequately protect PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PII going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Award Plaintiff and the Class actual and statutory damages, punitive damages, nominal damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 11, 2023

Respectfully submitted,

/s/ Leonard A. Bennett

Leonard A. Bennett, VSB #37523
Craig C. Marchiando, VSB #89736
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Blvd., Ste. 1-A
Newport News, VA 23601
Telephone: (757) 930-3660
Facsimile: (757) 930-3662
Email: lenbennett@clalegal.com
Email: craig@clalegal.com

Drew D. Sarrett, VSB #81658
CONSUMER LITIGATION ASSOCIATES, P.C.
626 E. Broad Street, Suite 300
Richmond, Virginia 23219
Phone: (804) 905-9900
Facsimile: (757) 930-3662
Email: drew@clalegal.com

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

Attorneys for Plaintiff